

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-301241

(43)Date of publication of application : 13.12.1990

(51)Int.Cl.

H04L 9/06
G06F 13/00
G09C 1/00
H04L 9/14

(21)Application number : 01-121861

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 15.05.1989

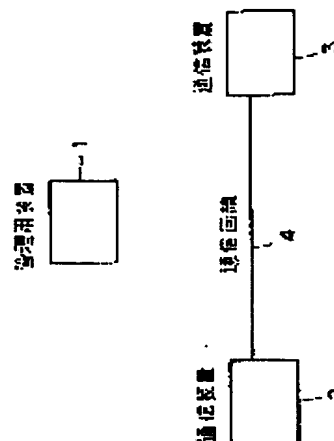
(72)Inventor : KOBAYASHI TETSUJI

(54) DELIVERY SYSTEM FOR COMMON KEY

(57)Abstract:

PURPOSE: To eliminate the need for an open public table and to sufficiently protect the secrecy of a communication equipment by providing a power cryptographic equipment to each communication equipment and using the power cryptographic equipment.

CONSTITUTION: A management equipment 1 gives public information in common to the communication system and secret information generated corresponding to the public identification information of the communication equipment 1 to each communication equipment and each communication equipment stores the public information and the secret information. When the power cryptographic equipment is used to deliver the common key, the public information in common to the communication system and the secrecy information for each communication equipment are used for the text to be sent and a communication equipment 2 gives a digital signature to apply the transmission to the communication equipment 3. The communication equipment 3 confirms the adequacy of the received digital signature, adds the digital signature of the communication equipment 3 to other text relating to the delivery of the common key, sends the result to the communication equipment 2, and the communication equipment 2 confirms the adequacy of the digital signature to confirm the adequacy of the communication equipment 3. Since the management equipment cannot recognize the common key, the secrecy of the common key of the communication equipment is maintained.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A) 平2-301241

⑬ Int.Cl.¹

識別記号

庁内整理番号

⑭ 公開 平成2年(1990)12月13日

H 04 L 9/06
G 06 F 13/00
G 09 C 1/00
H 04 L 9/14

3 5 1 E

7459-5B
7343-5B

6945-5K H 04 L 9/02

Z

審査請求 未請求 請求項の数 1 (全12頁)

⑮ 発明の名称 共通鍵の配送方式

⑯ 特 願 平1-121861

⑰ 出 願 平1(1989)5月15日

⑱ 発 明 者 小 林 哲 二 東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内

⑲ 出 願 人 日本電信電話株式会社 東京都千代田区内幸町1丁目1番6号

⑳ 代 理 人 弁理士 草 野 卓

明 細 書

1. 発明の名称

共通鍵の配送方式

2. 特許請求の範囲

(i) 一つ以上の管理用装置と、二つ以上の通信装置により構成される通信システムにおいて、
一つの管理用装置が、通信システムで共通な公開情報および通信装置の識別用の公開識別情報を用いて生成した秘密情報を、各通信装置に付与し、各通信装置は、通信システムで共通な公開情報および通信装置ごとの秘密情報を保持する第1の過程、および、

二つ以上の通信装置が、べき乗暗号装置を用いて共通鍵の配送を行うときに、送るべき電文の1つに対し、上記通信システムで共通な公開情報および通信装置ごとの秘密情報を用いて、各通信装置がディジタル署名を付与することにより、互いに相手側通信装置から受信した電文の正当性確認を行う第2の過程、を有することを特徴とする共通鍵の配送方式。

3. 発明の詳細な説明

「産業上の利用分野」

この発明は、通信回線により通信を行う二つ以上の通信装置の間で、共有する暗号鍵（即ち、共通鍵）をべき乗暗号装置を用いて配送する共通鍵の配送方式に関するものである。なおここで通信装置は、通信機能を有する装置、すなわち、電子計算機、端末装置、電子交換機、通信制御装置、通信処理装置、またはICカード、などを表すとする。

「従来の技術」

通信装置の間で秘密情報の通信を安全に行うためには、暗号を用いる通信が有効である。暗号法には暗号鍵と公開鍵暗号があることが知られている。暗号鍵では暗号鍵の配送が必要である。暗号鍵には、暗号化用の鍵である暗号化鍵と、復号化用の鍵である復号化鍵がある。暗号鍵は、暗号化鍵と復号化鍵が同一な暗号法を意味する。二つ以上の通信装置で共有する暗号鍵を、共通鍵と呼ぶ。暗号鍵の暗号アルゴリズムには、例え

ば、DES暗号("Data Encryption Standard", Federal Information Processing Standards Publication 46, U.S.A., (1977年))、及びFEAL-8暗号(宮口ほか著:"FEAL-8暗号アルゴリズム", 研究実用化報告, 第37巻第4/5号, (1988年))などがある。公開鍵暗号のアルゴリズムには、例えば、RSA暗号("R. L. Rivest他著:A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol. 21, No. 2, pp. 120-126, (1978年))、Rabin暗号("M. Rabin 著: Digitalized Signatures and Public-Key Cryptosystems", MIT/LCS/TR-212, Technical Report, MIT(1979年))などがある。

複数の通信装置では、公開鍵系の手法により、事前に秘密情報を共有することなく通信メッセージ(即ち、電文)に、ペキ乗暗号装置を用いて共通鍵の配送または生成を行う方式が既に知られている。その第1に、二重暗号を用いる方式(例えば、「小林哲二著:"暗号通信における二重暗号

型鍵配送方式", 電子情報通信学会論文誌, Vol. J71-D, No. 9, pp. 1815-1822, (1988年))における基本処理手順を参照)である。第2に、Diffie-Hellmanによる共通鍵配送方式(例えば、"New Directions in Cryptography", IEEE Transactions, Information Theory, IT-22, pp. 644-654 (1976年)を参照)である。第3に、公開鍵暗号(例えば、RSA暗号、Rabin暗号)などである。公開鍵系の手法を用いた共通鍵配送では、公開された情報の安全性を確保するために、公開鍵の管理を行う必要があるのが欠点である。このための対策として、通信システム内で通信装置を一意に識別できる公開識別情報(即ち、通信システム内で一意に付与された公開の識別情報であり、例えば、電話番号、住所、通信装置識別子、など)を用いる方式がある。デジタル署名は、メッセージの作成者とメッセージ内容の正当性を保証する機能である。公開識別情報に基づくデジタル署名の安全な方式として、Fiat-Shamirによる方式(A. Fiat and A. Shamir著:"How To Prove

Yourself: Practical Solutions to Identification and Signature Problems", Proceedings of CRYPTO 86, Springer-Verlag, Lecture Notes in Computer Science 263, pp. 186-194(1987年))が提案されているが、その方法では共通鍵の配送はできない。

「発明が解決しようとする課題」

従来に提案されている公開識別情報を用いる共通鍵配送方式では、管理用装置が通信装置の共通鍵を知ることができること等の秘密保護に問題がある。この発明の目的は、複数の通信装置間における共通鍵の配送において、公開鍵を不要とし、かつ通信装置の秘密保護が十分な共通鍵の配送方式を提供することである。

「課題を解決するための手段」

この発明は、一つ以上の管理用装置と、複数の通信装置により構成される通信システムに適用する。各通信装置は、通信システム内で一意に定まる公開識別情報を有することとする。各通信装置は、ペキ乗暗号装置を備えている。ペキ乗暗号装

置を用いることにより、複数の通信装置の間では、事前に秘密情報を共有することなく共通鍵の配送を行うことができる。通信装置の間の共通鍵の配送は、次の二つの独立な過程により実現する。

①共通鍵配送の第1の過程:

各通信装置が管理用装置に登録する時に、管理用装置は、通信システムで共通な公開情報と、通信装置の公開識別情報に対応して生成した秘密情報を、各通信装置に付与し、各通信装置はそれらの公開情報と秘密情報を保持する。なお、管理用装置は、個々の通信装置対応に生成した秘密情報を、通信装置に付与した後では、保持する必要はない。

②共通鍵配送の第2の過程:

管理用装置からそれぞれ秘密情報を得て保持している複数の通信装置(例えば、通信装置aと通信装置b)が、共通鍵の配送を行うときに、通信装置aは、共通鍵の配送に関連した電文に、デジタル署名を付加し、通信装置bに送信する。通信装置bは受信したデジタル署名の正当性を確認

する。更に、通信装置bは、共通鍵の配送に関した別の電文に、通信装置bのデジタル署名を付加し、通信装置aに送信する。通信装置aは、デジタル署名の正当性を確認することにより、通信装置bの正当性を確認する。また、これらの電文から、各通信装置は共通鍵を共有する。ここで、電文の数、電文内容、およびデジタル署名の対象とするデータは、共通鍵を配送する方式により、異なっている。この共通鍵を配送する方式としては従来より知られているベキ乗暗号装置を用いる各種の共通鍵配送方式を利用できる。

「作用」

前述の手段において、通信装置の間で共有する共通鍵の値は、管理用装置では生成できないので、管理用装置は、共通鍵を知ることができないため、通信装置の共通鍵の秘密が保たれている。また、公開鍵は不要である。

「実施例」

第1図は、この発明が適用される通信システムの一構成例であり、管理用装置1、通信装置2、

通信装置3、通信装置4で構成されている。通信装置が、二つ以上ある場合も同様である。次に、記法を述べる。整数は、この発明の実施例では、負でない整数を意味する。A、B、t及びNを任意の整数とすると、BについてのNを法とする剰余がAであることを、 $A = B \bmod N$ と表す。AとBがNを法として合同であることを、 $A \equiv B \pmod{N}$ と表す。Aのt乗の法をNとする剰余である、 $A^t \bmod N$ を、 $\exp(A, t) \bmod N$ と表す。||は、二つ以上のデータのそのままの値の連結を表す。⊕は排他的論理和の演算を表す。

通信装置wの公開鍵情報、ID_wとする。ここで、wは任意の値であり、例えば、通信装置aの識別子はID_a、通信装置bの識別子はID_bとなる。公開鍵情報は、通信システム内では、一意に定まるとする。

次に、ベキ乗暗号装置について述べる。各通信装置は、ベキ乗暗号装置を備えるものとする。整数のパラメータを、平文をM、暗号文をC、暗号化鍵をK、復号化鍵をKI、公開の整数をpとす

ると、

$$C = \exp(M, K) \bmod p$$

$$M = \exp(C, KI) \bmod p$$

となる。ここで、 $0 \leq M < p$ 、 $0 \leq C < p$ 、かつ

$$K \cdot KI \equiv 1 \pmod{\phi(p)}$$

である。 $\phi(\cdot)$ は、オイラーの関数である。即ち、pの素因数を、P、Q、R、・・・とすると、

$$p = P^a \cdot Q^b \cdot R^c \cdots$$

であるから、

$$\phi(p) = p(1-1/P)(1-1/Q)(1-1/R) \cdots$$

である。したがって、pが素数のときは、

$$\phi(p) = p - 1$$

である。ベキ乗暗号装置は、ハードウェア、又はハードウェアとソフトウェアの組み合わせにより実現できる。ベキ乗暗号装置における、ベキ乗剰余、および逆数の計算法などには、任意の方法を利用できる。それらの計算法は、例えば、「絶野はか著“現代暗号理論”、電子情報通信学会、(1985年)」などに述べられている。

第2図は、ベキ乗暗号装置11の一構成例であ

る。信号路12は、ベキ乗暗号装置11へ入力データを入力するための信号路であり、任意の整数のデータMを入力する。信号路13は鍵(暗号化鍵または復号化鍵)の入力のための信号路であり、暗号化鍵Kを入力する例を示してある。信号路14は法の値pの入力のための信号路である。ベキ乗暗号装置11は、入力データMについて、暗号化鍵Kの値を指数とするベキ乗の法の値pによる剰余を計算して、信号路15から出力データCを出力する。ここで、 $C = \exp(M, K) \bmod p$ である。

ベキ乗暗号装置16は、ベキ乗暗号装置11と同じ装置であり、復号化鍵KIを鍵として入力している例である。信号路17から入力された暗号文Cは、ベキ乗暗号装置16により復号されて、信号路20から平文Mを出力する。

第3図は、ベキ乗暗号装置21の一構成例である。ベキ乗暗号装置21は、ベキ乗暗号装置11、16とは異なる型のベキ乗暗号装置である。この型のベキ乗暗号装置では、整数のパラメータを、

H、t、pとすると、

$$J = \exp(H, t) \bmod p$$

となる。ここで、 $0 < J < p$ 、 $0 < H < p$ 、かつ
 $0 \leq t < p$ 、である。即ち、信号路23からは、
 整数Hを入力する。信号路24からは、法の値p
 を入力する。信号路22からデータtを入力して、
 データHおよび法の値pを用いて、信号路25か
 ら、出力データJを出力する。

次に、管理用装置と通信装置で使用する関数f
 (・)について述べる。関数f(・)は、任意の数値
 θを、

$$0 \leq f(\theta) < n$$

の値に変換する関数であり、f(θ)からθを求
 めるのは、計算時間から見て困難であるとする。
 f(・)は、例えば、次のようにして実現できる。
 θは、長さがn未満のときは、必要により、0を
 後に付加して、θの長さがnになるようにし、か
 つ個々のθ_i、 $i = 1, 2, \dots, m$ は暗
 号装置のブロック長になるように選択して、

$$\theta = \theta_1 \parallel \theta_2 \parallel \dots \parallel \theta_m$$

まず、管理用装置は、各通信装置が管理用装置
 に登録を行うときに、次の共通鍵配送の第1の過
 程を実行する。

共通鍵配送の第1の過程：

ステップ 1：

管理用装置は、管理用装置の秘密情報として、
 素数α、βを生成し保持する。次に、

$$n = \alpha \cdot \beta$$

を計算する。nは公開情報である。次に、公開情
 報として、一つ以上の素数を生成し、それから整
 数pを作成し、保持する。次に、公開の関数であ
 る、f(・)の形式を定める。次に、Fiat-Shamir
 方式のパラメータである、tとkの値を定める。
 (ステップ1は、一度行えば、ステップ2～ステ
 ップ4の異なる通信装置への処理に対しても共通
 である。)

ステップ 2：

任意の通信装置wについての公開鍵情報をも、
 ID_wとする。管理用装置は、通信装置wからの
 依頼により、j = 1, 2, ..., Kについて、

と分解する。Tを公開のデータとする。E(Z1,
 U)を、任意のデータUを暗号装置により、鍵Z1
 を用いて暗号化した値とする。この暗号装置には、
 任意の暗号アルゴリズム(例えば、前述した、
 FEAL-8暗号、DES暗号、RSA暗号など)を使
 用可能である。すると、

$$P_1 = E(\theta_1, T) \oplus T$$

$$P_2 = E(\theta_2, P_1) \oplus P_1$$

...

$$P_m = E(\theta_m, P_{m-1}) \oplus P_{m-1}$$

とし、

$$f(\theta) = P_1 \parallel P_2 \parallel \dots \parallel P_m$$

とすることができる。以下では、共通鍵配送の実
 施例を四つ述べる。

[共通鍵配送の実施例1]

二重暗号の基本処理手順による共通鍵配送に、
 Fiat-Shamir方式によるデジタル署名を適用し
 て、通信装置で相互に相手側の正当性の認証を行
 う場合について示す。ペキ乗暗号装置は、第2図
 の型のペキ乗暗号装置を用いる。

$$V_{w,j} = f(ID_w, j)$$

を計算する。ここで、V_{w,j}は、nを法とする平方
 剰余であるように、j = 1, 2, ..., kを選
 択する。次に、j = 1, 2, ..., kについて、
 管理用装置と、通信装置wの秘密情報である、

$$S_{w,j} = (1/V_{w,j})^{1/2} \bmod n$$

を求める。ここで、S_{w,j}は、1/V_{w,j}の法をnと
 する最小平方根とする。

ステップ 3：

管理用装置は、通信装置wに、秘密情報として、
 S_{w,j}、(j = 1, 2, ..., k)
 を与える。公開情報である、nとpの値、および
 f(・)の形式も与える。pが合成数のときは、そ
 の素因数も与える。Fiat-Shamir方式のパラメー
 タである、tとkの値も与える。

ステップ 4：

管理用装置は、通信装置wに与えるために生成
 したV_{w,j}とS_{w,j}、(j = 1, 2, ..., k)、
 の値を、管理用装置から消去する。

次に、第1の過程により、管理用装置から、公

開情報、および秘密情報を得た通信装置は、任意の時点で共通鍵配送の第2の過程により、共通鍵の配送を行う。

第4図は、共通鍵配送の第2の過程における電文の送信例である。

共通鍵配送の第2の過程では、通信装置aが共通鍵配送を開始する場合を述べる。(通信装置bが共通鍵配送を開始する場合も同様である)。

共通鍵配送の第2の過程:

ステップ 1:

通信装置aは、通信装置aと通信装置bの共通鍵 K_{ab} を生成する。次に、二重暗号の暗号化鍵 K_e を乱数により生成する。次に、復号化鍵 K_d を、

$$K_d = 1/K_e \bmod \phi(p)$$

により求める。次に、

$AS1 = \exp(K_{ab} \parallel ID_a, K_e) \bmod p$ を計算する。次に、乱数 $R_{a,i}$ ($i=1, 2, \dots, t$)、を生成し、

$$X_{a,i} = (R_{a,i})^2 \bmod n, (i=1, 2, \dots, t)$$

デジタル署名である。

ステップ 2:

通信装置bは、A1を含む電文1を受信する。

次に、 $j=1, 2, \dots, k$ について、

$$V_{a,j} = f(ID_a \parallel j)$$

を計算する。次に、 $i=1, 2, \dots, t$ について、

$$Z_{a,i} = (Y_{a,i})^2 \prod V_{a,j} \bmod n$$

$$G_{a,j,i} = 1, \text{ for } j=1, 2, \dots, k$$

を計算する。次に、

$$G_a = f(AS1 \parallel Z_{a,1} \parallel Z_{a,2} \parallel \dots \parallel Z_{a,t})$$

の先頭 $k \cdot t$ ビット

が成立することにより、通信装置aのデジタル署名の正当性を検証する。成立しないときは異常終了する。

次に、二重暗号の暗号化鍵 K_e を乱数により生成する。次に、復号化鍵 K_d を、

$$K_d = 1/K_e \bmod \phi(p)$$

により、求める。次に、

$$AS2 = \exp(AS1, K_e) \bmod p$$

$$= \exp(K_{ab} \parallel ID_a, K_e \cdot K_e) \bmod p$$

を求める。次に、 $f(AS1 \parallel X_{a,1} \parallel X_{a,2} \parallel \dots \parallel X_{a,t})$ の先頭 $k \cdot t$ ビット、を求め、その $k \cdot t$ ビットの個々のビットを、

$$G_a = \{G_{a,i,j}, (i=1, 2, \dots, t; j=1, 2, \dots, k)\}$$

の個々のビットとする。即ち、 $G_{a,i,j}$ の要素は、

$$\{G_{a,1,1}, G_{a,1,2}, \dots, G_{a,1,k}, G_{a,2,1}, G_{a,2,2}, \dots, G_{a,2,k}\}$$

である。次に、 $i=1, 2, \dots, t$ について、

$$Y_{a,i} = R_{a,i} \cdot (\prod S_{a,j}) \bmod n$$

$$G_{a,j,i} = 1, \text{ for } j=1, 2, \dots, k$$

を計算する。ここで、

$$\prod S_{a,j} = 1, \text{ for } j=1, 2, \dots, k$$

は、 $j=1, 2, \dots, k$ について、 $G_{a,j,i} = 1$ である $S_{a,j}$ の積を表す。次に、

$$Y_a = Y_{a,1} \parallel Y_{a,2} \parallel \dots \parallel Y_{a,t}$$

とする。次に、

$$A1 = \{ID_a, AS1, G_a, Y_a\}$$

を求め、A1を含む電文1を通信装置bに送信する。ここで、 G_a, Y_a が電文AS1に対するデ

ジタル署名である。次に、乱数 $R_{b,i}$ ($i=1, 2, \dots, t$)、を生成し、

$$X_{b,i} = (R_{b,i})^2 \bmod n, (i=1, 2, \dots, t)$$

を計算する。次に、 $f(AS2 \parallel X_{b,1} \parallel X_{b,2} \parallel \dots \parallel X_{b,t})$ の先頭 $k \cdot t$ ビット、を求め、その $k \cdot t$ ビットの個々のビットを、

$$G_b = \{G_{b,i,j}, (i=1, 2, \dots, t; j=1, 2, \dots, k)\}$$

の個々のビットとする。即ち、 $G_{b,i,j}$ の要素は、

$$\{G_{b,1,1}, G_{b,1,2}, \dots, G_{b,1,k}, G_{b,2,1}, G_{b,2,2}, \dots, G_{b,2,k}\}$$

である。次に、 $i=1, 2, \dots, t$ について

$$Y_{b,i} = R_{b,i} \cdot (\prod S_{b,j}) \bmod n$$

$$G_{b,j,i} = 1, \text{ for } j=1, 2, \dots, k$$

を計算する。次に、

$$Y_b = Y_{b,1} \parallel Y_{b,2} \parallel \dots \parallel Y_{b,t}$$

を作成する。次に、

$$A2 = \{ID_b, AS2, G_b, Y_b\}$$

を作成し、A2を含む電文2を通信装置aに送信する。ここで、 G_b, Y_b が、電文AS2に対する通信装置bのデジタル署名である。

ステップ 3:

通信装置 a は、A2 を含む電文 2 を受信する。

次に、

$$V_{j,1} = f(1D, 1j), \quad j=1, 2, \dots, k$$

を計算する。次に、 $j=1, 2, \dots, k$ について、

$$Z_{j,1} = (Y_{j,1})^2 \prod_{G_{j,1}=1} V_{j,1} \bmod a$$

を計算する。次に、

$$G_i = f(AS2 \parallel Z_{1,1} \parallel Z_{2,1} \parallel \dots \parallel Z_{k,1})$$

の先頭 $k \cdot t$ ビット

が成立することにより、通信装置 b のデジタル署名の正当性を検証する。成立しないときは異常終了する。次に、

$$A3 = \exp(AS2, K1, 1) \bmod p$$

$$= \exp(KC_{a,1} \parallel 1D, K, 1) \bmod p$$

を計算し、A3 を含む電文 3 を通信装置 b に送信する。

ステップ 4:

通信装置 b は、A3 を含む電文 3 を受信する。

次に、

$$n = \alpha \cdot \beta$$

を計算する。n は公開情報である。次に、公開情報として、素数 H を生成し、保持する。次に、公開の関数である、 $f(\cdot)$ の形式を定める。次に、Flat-Shamir 方式のパラメータである、 l と k の値を定める。

(ステップ 1 は、一度行えば、ステップ 2 ~ ステップ 4 の異なる通信装置への処理に対しても共通である。)

ステップ 2:

任意の通信装置 w についての公開識別情報を、 $1D_w$ とする。管理用装置は、通信装置 w からの依頼により、 $j=1, 2, \dots, K$ について、

$$V_{j,w} = f(1D_w, 1j)$$

を計算する。ここで、 V_j は、n を法とする平方剰余であるように、 $j=1, 2, \dots, k$ を選択する。次に、 $j=1, 2, \dots, k$ について、管理用装置と、通信装置 w の秘密情報である、

$$S_{j,w} = (1/V_{j,w})^{1/2} \bmod n$$

を求める。ここで、 $S_{j,w}$ は、 $1/V_{j,w}$ の法を n と

$$A4 = \exp(A3, K1, 1) \bmod p$$

$$= KC_{a,1} \parallel 1D,$$

を得る。次に $1D$ が正しいかどうかを確認し、正しいときは、共通鍵 $KC_{a,1}$ を保持する。 $1D$ が正しくないときは異常終了する。

以上の共通鍵配送の過程において、異常が発生時は、その過程は異常終了する。

[共通鍵配送の実施例 2]

Biffin-Hellman による共通鍵配送の方式に、

Flat-Shamir 方式によるデジタル署名を適用して、通信装置で相互に相手側の正当性の検証を行う場合について示す。ペキ乗暗号装置は、第 3 図のペキ乗暗号装置を用いる。

まず、管理用装置は、各通信装置が管理用装置に登録を行うときに、次の共通鍵配送の第 1 の過程を実行する。

共通鍵配送の第 1 の過程:ステップ 1:

管理用装置は、管理用装置の秘密情報として、素数 α 、 β を生成し保持する。次に、

する最小平方根とする。

ステップ 2:

管理用装置は、通信装置 w に、秘密情報として、 $S_{j,w}$ 、($j=1, 2, \dots, k$)

を与える。また公開情報である、 $n f(\cdot)$ 、H も与える。Flat-Shamir 方式のパラメータである、 l と k の値も与える。

ステップ 4:

管理用装置は、通信装置 w に与えるために生成した $V_{j,w}$ と $S_{j,w}$ 、($j=1, 2, \dots, k$)、の値を、管理用装置から消去する。

次に、第 1 の過程により、管理用装置から、公開情報、および秘密情報を得た通信装置は、任意の時点で共通鍵配送の第 2 の過程により、共通鍵の配送を行う。

第 5 図は、共通鍵配送の第 2 の過程における電文の交換例である。

共通鍵配送の第 2 の過程では、通信装置 a が鍵配送を開始する場合を述べる。(通信装置 b が鍵配送を開始する場合も同様である)。

共通鍵配送の第2の過程:ステップ 1:

通信装置 a は、秘密情報 T_a を乱数により生成する。次に、

$$W_a = \exp(H, T_a) \bmod p$$

を求める。次に、乱数 R_{a,i} (i=1, 2, ..., t) を生成し、

$$X_{a,i} = (R_{a,i})^2 \bmod n, (i=1, 2, \dots, t)$$

を求める。次に、f(W_a || X_{a,1} || X_{a,2} || ... || X_{a,t}) の先頭 k・t ビット、を求め、その k・t ビットの個々のビットを、

$$G_{a,i} = \{G_{a,i,j}\}, (i=1, 2, \dots, t; j=1, 2, \dots, k)$$

の個々のビットとする。次に、i=1, 2, ..., t について、

$$Y_{a,i} = R_{a,i} \cdot (\prod S_{a,j}) \bmod n \\ G_{a,i,j} = 1, \text{ for } j=1, 2, \dots, k$$

を計算する。次に、

$$Y_a = Y_{a,1} || Y_{a,2} || \dots || Y_{a,t}$$

とする。次に、

$$KCQ_{a,b} = \exp((\exp(H, T_a) \bmod p), T_b) \bmod p \\ = \exp(K, T_a, T_b) \bmod p$$

を計算する。次に、共通鍵 KC_{a,b} を、

$$KC_{a,b} = KCQ_{a,b} \text{ の先頭からの部分ビット (ビット長 L)}$$

により求め保持する。ビット長 L は、共通鍵のビット長である。次に、

$$W_b = \exp(H, T_b) \bmod p$$

を計算する。次に、乱数 R_{b,i} (i=1, 2, ..., t) を生成し、

$$X_{b,i} = (R_{b,i})^2 \bmod n, (i=1, 2, \dots, t)$$

を求める。次に、f(W_b || X_{b,1} || X_{b,2} || ... || X_{b,t}) の先頭 k・t ビット、を求め、その k・t ビットの個々のビットを、

$$G_b = \{G_{b,i,j}\}, (i=1, 2, \dots, t; j=1, 2, \dots, k)$$

の個々のビットとする。次に、i=1, 2, ..., t について、

$$Y_{b,i} = R_{b,i} \cdot (\prod S_{b,j}) \bmod n \\ G_{b,i,j} = 1, \text{ for } j=1, 2, \dots, k$$

$$B1 = (ID_a, W_a, G_a, Y_a)$$

を求め、B1 を含む電文 1 を通信装置 b に送信する。ここで、G_a、Y_a が共通鍵の配送に關した電文 W_a に対するデジタル署名である。

ステップ 2:

通信装置 b は、B1 を含む電文 1 を受信する。次に、通信装置 b は、秘密情報 T_b を乱数により生成する。次に、

$$V_{b,j} = f(ID_b, j), j=1, 2, \dots, k$$

を計算する。次に、i=1, 2, ..., t について、

$$Z_{a,i} = (Y_{a,i})^2 \prod V_{a,j} \bmod n \\ G_{a,i,j} = 1, \text{ for } j=1, 2, \dots, k$$

を計算する。次に、

$$G_a = f(W_a || Z_{a,1} || Z_{a,2} || \dots || Z_{a,t})$$

の先頭 k・t ビット

が成立することにより、通信装置 a のデジタル署名の正当性を検証し、成立しないときは異常終了する。次に、通信装置 b は秘密情報 T_b を乱数により生成し、

を計算する。次に、

$$Y_b = Y_{b,1} || Y_{b,2} || \dots || Y_{b,t}$$

とする。次に、

$$B2 = (ID_b, W_b, G_b, Y_b)$$

とする。次に、B2 を含む電文 2 を通信装置 a に送信する。ここで、G_b、Y_b が、共通鍵配送に關した電文 W_b に対する通信装置 b のデジタル署名である。

ステップ 3:

通信装置 a は、B2 を含む電文 2 を受信する。

次に、

$$V_{b,j} = f(ID_b, j), j=1, 2, \dots, k$$

を計算する。次に、i=1, 2, ..., t について、

$$Z_{b,i} = (Y_{b,i})^2 \prod V_{b,j} \bmod n \\ G_{b,i,j} = 1, \text{ for } j=1, 2, \dots, k$$

を計算する。次に、

$$G_b = f(W_b || Z_{b,1} || Z_{b,2} || \dots || Z_{b,t})$$

の先頭 k・t ビット

が成立することにより、通信装置 b のデジタル

署名の正当性を検証する。成立しないときは異常終了する。次に、

$$KC_{a,i} = \exp((\exp(E, T_a) \bmod p), T_a) \bmod p \\ = \exp(E, T_a, T_a) \bmod p$$

を計算し、

$$KC_{a,i} = KCQ_{a,i} \text{の先頭からの部分ビット(ビット長 } L)$$

とし、 $KC_{a,i}$ を保持する。

なお、以上の共通鍵配送の過程において、異常が発生時は、その過程は異常終了する。

[共通鍵配送の実施例3]

RSA暗号による鍵配送に、Flat-Shamir方式によるデジタル署名を適用して、通信装置で相互に相手側の正当性の認証と共通鍵の配送を行う場合について示す。ペキ乗暗号装置は、第2図のペキ乗暗号装置を用いる。

まず、管理用装置は、各通信装置が管理用装置に登録を行うときに、次の共通鍵配送の第1の過程を実行する。

共通鍵配送の第1の過程:

$$S_{w,j} = (1/V_{w,j})^{1/2} \bmod n$$

を求める。ここで、 $S_{w,j}$ は、 $1/V_{w,j}$ の法を n とする最小平方根とする。

ステップ3:

管理用装置は、通信装置 w に、秘密情報として、 $S_{w,j}$ ($j=1, 2, \dots, k$)を与える。また、公開情報である、 $n f(\cdot)$ も与える。Flat-Shamir方式のパラメータである、 i と k の値も与える。

ステップ4:

管理用装置は、通信装置 w に与えるために生成した $V_{w,j}$ 、 $S_{w,j}$ ($j=1, 2, \dots, k$)の値を、管理用装置から消去する。

次に、第1の過程により、管理用装置から、公開情報、および秘密情報を得た通信装置は、任意の時点で共通鍵配送の第2の過程により、共通鍵の配送を行う。

第6図は、共通鍵配送の第2の過程における電文の交換例である。

共通鍵配送の第2の過程では、通信装置 a が鍵

ステップ1:

管理用装置は、管理用装置の秘密情報として、素数 α 、 β を生成し保持する。次に、

$$n = \alpha \cdot \beta$$

を計算する。 n は公開情報である。次に、公開の関数である、 $f(\cdot)$ の形式を定める。次に、Flat-Shamir方式のパラメータである、 i と k の値を定める。

(ステップ1は、一度行えば、ステップ2～ステップ4の異なる通信装置への処理に対しても共通である。)

ステップ2:

任意の通信装置 w についての公開鍵情報、 ID_w とする。管理用装置は、通信装置 w からの依頼により、 $j=1, 2, \dots, k$ について、

$$V_{w,j} = f(ID_w, j)$$

を計算する。ここで、 $V_{w,j}$ は、 n を法とする平方剰余であるように、 $j=1, 2, \dots, k$ を選択する。次に、 $j=1, 2, \dots, k$ について、管理用装置と、通信装置 w の秘密情報である、

配送を開始する場合を述べる。(通信装置 b が鍵配送を開始する場合も同様である。)

共通鍵配送の第2の過程:

ステップ0:

通信装置 a は、RSA暗号の公開鍵(暗号化鍵) PK_a 、秘密の素数 P_a 、 Q_a 、公開の整数 N_a 、および秘密鍵(復号化鍵) SK_a を生成する。

$$N_a = P_a \cdot Q_a$$

であり、 P_a と Q_a は通信装置 a の秘密の素数である。また、

$$PK_a \cdot SK_a \equiv 1 \pmod{\phi(N_a)}$$

である。通信装置 a は、 PK_a 、 N_a 、 SK_a 、 P_a 、 Q_a を保持する。

(ステップ0は、一度行っておけば、以後に共通鍵配送の第2の過程を再び行うときは、省略できる。)

ステップ1:

通信装置 a は、乱数 $R_{a,i}$ ($i=1, 2, \dots, t$)を生成し、

$$X_{a,i} = (R_{a,i})^2 \bmod n, (i=1, 2, \dots, t)$$

を計算する。次に、 $f(PK_a, \|N_a\|X_{a,1}\|X_{a,2}\|\cdots\|X_{a,t})$ の先頭 $k \cdot t$ ビット、を求め、その $K \cdot t$ ビットの個々のビットを、

$$G_a = \{G_{a,i}, (i=1, 2, \dots, t; j=1, 2, \dots, k)\}$$

の個々のビットとする。次に、 $i=1, 2, \dots, t$ について、

$$Y_{a,i} = R_{a,i} \cdot (\prod S_{a,j}) \bmod n$$

$$G_{a,i,j} = 1, \text{ for } j=1, 2, \dots, k$$

を求める。次に、

$$Y_a = Y_{a,1}\|Y_{a,2}\|\cdots\|Y_{a,t}$$

とする。次に、

$$C1 = \{ID_a, PK_a, N_a, G_a, Y_a\}$$

とする。次に $C1$ を含む電文 1 を通信装置 b に送信する。ここで、 G_a, Y_a が電文 PK_a に対する通信装置 a のデジタル署名である。

ステップ 2:

通信装置 b は、 $C1$ を含む電文 1 を受信する。

次に、通信装置 b は、

$$V_{a,j} = f(ID_a, \|j\|), j=1, 2, \dots, k$$

$$Y_{a,i} = R_{a,i} \cdot (\prod S_{a,j}) \bmod n$$

$$G_{a,i,j} = 1, \text{ for } j=1, 2, \dots, k$$

を計算する。次に、

$$C2 = \{ID_b, W1, G_a, Y_a\}$$

を求め、 $C2$ を含む電文 2 を、通信装置 a に送信する。ここで、 G_a, Y_a が、電文 $W1$ に対する通信装置 b のデジタル署名である。

ステップ 3:

通信装置 a は、 $C2$ を含む電文 2 を受信する。

次に、

$$V_{a,j} = f(ID_a, \|j\|), j=1, 2, \dots, k$$

を計算する。次に、 $i=1, 2, \dots, t$ について、

$$Z_{a,i} = (Y_{a,i})^2 \prod V_{a,j} \bmod n$$

$$G_{a,i,j} = 1, \text{ for } j=1, 2, \dots, k$$

を計算する。次に、

$$G_a = f(W_a, \|Z_{a,1}\|Z_{a,2}\|\cdots\|Z_{a,t})$$

の先頭 $k \cdot t$ ビット

が成立することにより、通信装置 b のデジタル署名の正当性を検証する。成立しないときは異常終了する。次に、

を計算し、 $i=1, 2, \dots, t$ について、

$$Z_{a,i} = (Y_{a,i})^2 \prod V_{a,j} \bmod n$$

$$G_{a,i,j} = 1, \text{ for } j=1, 2, \dots, k$$

を求める。次に、

$$G_a = f(PK_a, \|N_a\|Z_{a,1}\|Z_{a,2}\|\cdots\|Z_{a,t})$$

の先頭 $k \cdot t$ ビット

が成立することにより、通信装置 a のデジタル署名を検証し、成立しないときは、異常終了する。

次に、共通鍵 $KC_{a,b}$ を生成し、

$$W1 = \exp(KC_{a,b}, PK_a) \bmod N_a$$

を求める。次に、乱数 $R_{a,i}, (i=1, 2, \dots, t)$ 、を生成し、

$$X_{a,i} = (R_{a,i})^2 \bmod n$$

を求める。次に $f(W1\|X_{a,1}\|X_{a,2}\|\cdots\|X_{a,t})$ の先頭 $k \cdot t$ ビット、を求め、その $k \cdot t$ ビットの個々のビットを、

$$G_a = \{G_{a,i}, (i=1, 2, \dots, t; j=1, 2, \dots, k)\}$$

の個々のビットとする。次に、 $i=1, 2, \dots, t$ について、

$$Z2 = \exp(W1, SK_a) \bmod N_a$$

$$= \exp(KC_{a,b}, PK_a \cdot SK_a) \bmod N_a$$

$$= KC_{a,b}$$

を求め、これにより共通鍵 $KC_{a,b}$ を得て保持する。

なお、以上の共通鍵配送の過程において、異常が発生時は、その過程は異常終了する。

【共通鍵配送の実施例 4】

二重暗号の基本処理手順による共通鍵配送に、Flat-Shamir 方式によるデジタル署名を適用して、通信装置で相互に相手側の正当性の認証を行う場合について、実施例 1 とは別の実施例を示す。デジタル署名を実施例 1 とは別の電文に適用する例である。ペキ乗暗号装置は、第 2 図の型のペキ乗暗号装置を用いる。

まず、管理用装置は、各通信装置が管理用装置に登録を行うときに、次の共通鍵配送の第 1 の過程を実行する。

共通鍵配送の第 1 の過程:

共通鍵配送の実施例 1 の、共通鍵配送の第 1 の過程と同じである。

共通鍵配送の第2の過程:

ステップ 1:

通信装置 a は、通信装置 a と通信装置 b の共通鍵 K_{ab} を生成する。次に、二重暗号の暗号化鍵 K を乱数により生成する。更に、復号化鍵 KI を、

$$KI = 1/K \pmod{\phi(p)}$$

により求められる。次に、

$$A1 = \exp(KC_{ab} \parallel ID_a, K) \pmod{p}$$

を計算し、 $A1$ を含む電文 1 を通信装置 b に送信する。

ステップ 2:

通信装置 b は、 $A1$ を含む電文 1 を受信する。次に、二重暗号の暗号化鍵 K を乱数により生成する。次に、復号化鍵 KI を、

$$KI = 1/K \pmod{\phi(p)}$$

により求める。次に、

$$\begin{aligned} AS2 &= \exp(A1, KI) \pmod{p} \\ &= \exp(KC_{ab} \parallel ID_a, K \cdot KI) \pmod{p} \end{aligned}$$

を計算する。次に、乱数 $R_{i,j}$ ($i=1, 2, \dots$

次に、

$$V_{i,j} = f(ID_a \parallel j), \quad j=1, 2, \dots, k$$

を計算する。次に、 $i=1, 2, \dots, t$ について、

$$Z_{i,j} = (Y_{i,j})^2 \prod_{G_{i,j}=1} V_{i,j} \pmod{a}$$

を計算する。次に、

$$G_i = f(AS2 \parallel Z_{i,1} \parallel Z_{i,2} \parallel \dots \parallel Z_{i,k})$$

の先頭 $k \cdot t$ ビット

が成立することにより、通信装置 b のデジタル署名の正当性を検証する。成立しないときは異常終了する。次に、

$$\begin{aligned} AS3 &= \exp(AS2, KI) \pmod{p} \\ &= \exp(KC_{ab} \parallel ID_a, K) \pmod{p} \end{aligned}$$

を計算する。次に、乱数 R を生成し、

$$X_{i,j} = (R_{i,j})^2 \pmod{a}, \quad (i=1, 2, \dots, t)$$

を求める。次に、

$$G_i = f(AS3 \parallel X_{i,1} \parallel X_{i,2} \parallel \dots \parallel X_{i,k})$$

の先頭 $k \cdot t$ ビット

を求める。次に、 $i=1, 2, \dots, t$ につい

$\dots, t)$ を生成し、

$$X_{i,j} = (R_{i,j})^2 \pmod{a}, \quad (i=1, 2, \dots, t)$$

を計算する。次に、 $f(AS2 \parallel X_{i,1} \parallel X_{i,2} \parallel \dots \parallel X_{i,k})$ の先頭 $k \cdot t$ ビット、を求めその $k \cdot t$ ビットの個々のビットを、

$$G_i = \{G_{i,j}, \quad (i=1, 2, \dots, t; j=1, 2, \dots, k)\}$$

の個々のビットとする。次に、 $i=1, 2, \dots, t$ について、

$$\begin{aligned} Y_{i,j} &= R_{i,j} \cdot (\prod S_{i,j}) \pmod{a} \\ G_{i,j} &= 1, \text{ for } j=1, 2, \dots, k \end{aligned}$$

を計算する。次に、

$$Y_i = Y_{i,1} \parallel Y_{i,2} \parallel \dots \parallel Y_{i,k}$$

とする。次に、

$$A2 = \{ID_a, AS2, G_i, Y_i\}$$

とする。次に、 $A2$ を含む電文 2 を通信装置 a に送信する。ここで、 G_i, Y_i が、電文 $AS2$ に対する通信装置 b のデジタル署名である。

ステップ 3:

通信装置 a は、 $A2$ を含む電文 2 を受信する。

て、

$$\begin{aligned} Y_{i,j} &= R_{i,j} \cdot (\prod S_{i,j}) \pmod{a} \\ G_{i,j} &= 1 \text{ for } j=1, 2, \dots, k \end{aligned}$$

を計算する。 $Y_i = Y_{i,1} \parallel Y_{i,2} \parallel \dots \parallel Y_{i,k}$

とする。ここで、 G_i, Y_i が電文 $AS3$ に対する通信装置 a のデジタル署名である。次に、

$$A3 = \{ID_a, AS3, G_i, Y_i\}$$

を計算し $A3$ を含む電文 3 を通信装置 b に送信する。

ステップ 4:

通信装置 b は、 $A3$ を含む電文 3 を受信する。

次に、

$$V_{i,j} = f(ID_a \parallel j), \quad j=1, 2, \dots, k$$

を計算する。次に、 $i=1, 2, \dots, t$ について、

$$Z_{i,j} = (Y_{i,j})^2 \prod_{G_{i,j}=1} V_{i,j} \pmod{a}$$

を計算する。次に、

$$G_i = f(AS3 \parallel Z_{i,1} \parallel Z_{i,2} \parallel \dots \parallel Z_{i,k})$$

の先頭 $k \cdot t$ ビット

が成立することにより、通信装置 a のデジタル

署名を検証する。成立しないときは異常終了する。
成立したときは、

$$A4 = \exp(AS3, KI.) \bmod p \\ = KC..IID.$$

を計算し、IID.の正当性を確認し、異常のときは異常終了し、正当なときは、共通鍵KC..を得て保持する。

以上の共通鍵配送の過程において、異常が発生時は、その過程は異常終了する。なお、この発明では、以下の選択も可能である。

- ① この発明の適用に際して利用する通信網の物理的構成（例えば、専用線、交換回線、構内網など）、通信網インタフェース、及び通信プロトコルは、任意に選択できる。
- ② この発明の実施例では、ペキ乗暗号装置を用いた共通鍵配送にFlat-Shamir方式によるデジタル署名を適用する場合を記述したが、Flat-Shamir方式と類似の通信形態を有するデジタル署名方式（例えば、Flat-Shamir方式の、別のパラメータ選択の利用、拡張、改良）も、

れる。

- ② 通信装置は、共通鍵配送時に、管理用装置との通信が不要であるので、管理用装置と通信不能となっても、通信装置の間では暗号通信が可能である。

4. 図面の簡単な説明

第1図は通信システムの一構成例を示すブロック図、第2図はペキ乗暗号装置の一構成例を示すブロック図、第3図は第2図と異なるペキ乗暗号装置の一構成例を示すブロック図、第4図は共通鍵配送の実施例1の共通鍵配送第2の過程における電文の交信例を示す図、第5図は共通鍵配送の実施例2の共通鍵配送第2の過程における電文の交信例を示す図、第6図は共通鍵配送の実施例3の共通鍵配送第2の過程における電文の交信例を示す図である。

特許出願人 日本電信電話株式会社

代理人 草野 卓

この発明に適用できることは明らかであり、そのような場合もこの発明は含んでいる。

- ③ この発明の共通鍵配送の実施例3では、公開鍵暗号にRSA暗号を用いる場合を述べたが、Rabin暗号などの、他の公開鍵暗号も用いることが可能であり、この発明は、そのような場合も含んでいる。

- ④ 実施例では、管理用装置が1つの場合を述べたが、管理用装置が複数の場合も、各管理用装置の処理は同様である。その場合、管理用装置の秘密情報と公開情報を個別、または共通にすることにより、個々の管理用装置を独立させるか、または一体とするかを選択できる。

「発明の効果」

この発明の共通鍵配送方式は、次の長所がある。

- (i) 管理用装置の情報は、通信装置ではデジタル署名にのみ用いられるので、万一に第三者に漏洩しても、共通鍵が洩れないので安全性が高い。また、管理用装置は、共通鍵を知ることができないので、通信装置の共通鍵の秘密は保た

図 1

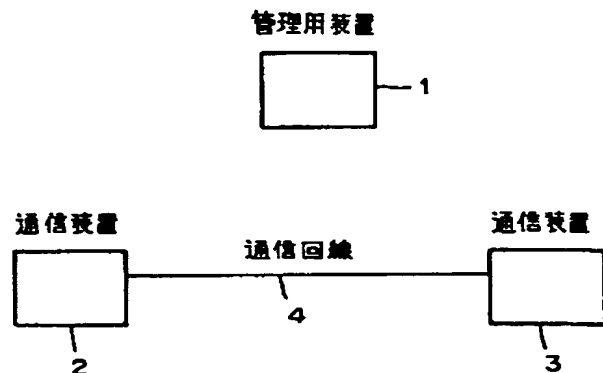


図 2

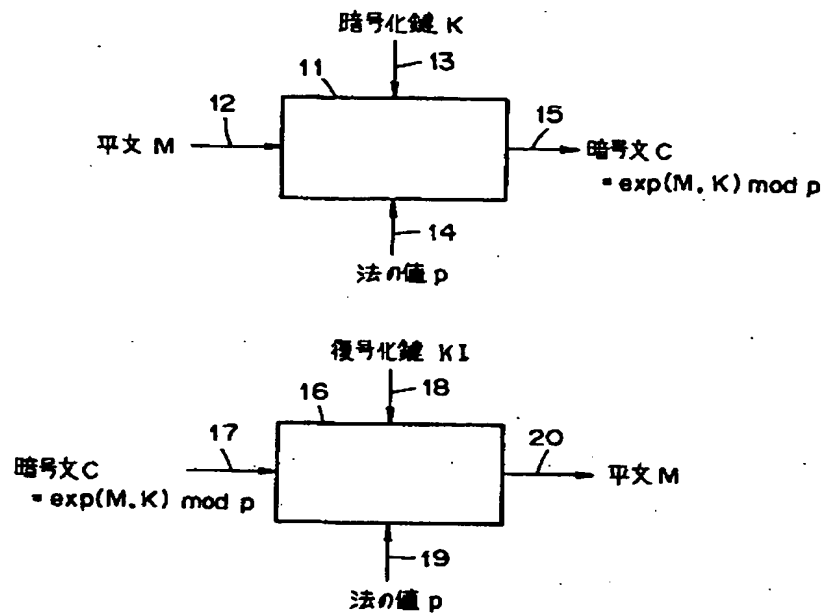


図 3

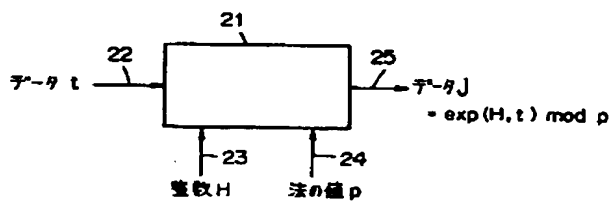


図 4

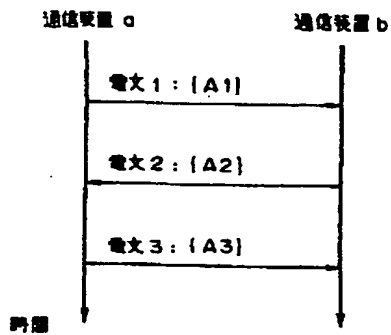


図 5

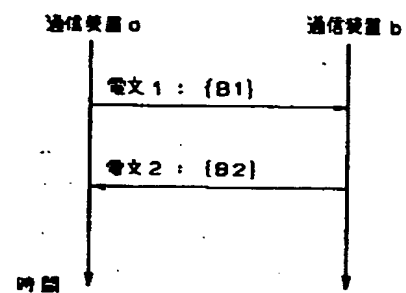


図 6

